The federal government believes that patient confidentiality is a basic Civil Right.

It allows patient information to be shared under strict controls, including with vendors who provide you with services that may require them to access patient information, or the systems that process, store, or transmit patient information, *even if they don't look at it*.

If you are a HIPAA Covered Entity, by law you are responsible for the compliance of your Business Associates.

If you are a Business Associate, by law you are responsible for the compliance of your Business Associate Subcontractors.

Not managing your relationships with Business Associates is a violation of federal law and can have severe consequences.

In 2016,

- **A hospital was fined $ 1.55 million for sharing Protected Health Information with a vendor without having signed a Business Associate Agreement.**
- **A medical practice was fined $ 750,000 for sharing Protected Health Information (PHI) with a vendor without having signed a Business Associate Agreement.**
- **A HIPAA Business Associate was fined $ 650,000 for breaching just 412 patient records**

In addition to the fines, those that were penalized also had to notify patients, incur legal fees, and suffer the effects of negative publicity and damage to their reputation and brand.

Vendors that will not sign off on their compliance, or believe that they do not have to comply, may create millions of dollars of risk to your organization. This should be quickly escalated to your management.

Use the following survey to validate that your vendors are complying. Personalize the survey with your contact information, and paste it into your letterhead template.

HIPAA BUSINESS ASSOCIATE COMPLIANCE Survey

We believe your organization is a HIPAA Business Associate. We are responsible to ensure you are compliant.
A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

In 2013 the HIPAA Omnibus Final Rule HIPAA required full compliance and data breach responsibility from Business Associates and their subcontractors. The included specific guidance related to technology.

Cloud Services and Data Centers (from a presentation by the HIPAA enforcement agency…)
Cloud service providers (and data centers, and online backup companies) are business associates if the data is maintained in the performance of its function even if the agreement with the covered entity does not contemplate any access or access only on a random or incidental basis. The test is persistence of custody, not the degree (if any) of access. Downstream entities that work at the direction of or on behalf of a business associate and handle PHI are required to comply with the applicable Privacy and Security Rule provisions, just like the "primary" business associate and are subject to the same liability for failure to do so.

***Computer equipment and copier manufacturers and service providers** are also business associates because the support and repair services they perform involve the handling of hard drives that store protected data*

***Encrypted data** is exempt from being reported as a data breach, but is not used to determine Business Associate status.*

Please answer the following questions and return them to us within 5 days.

Your Company Name: _____
Contact Name _____ Title _____
E-mail _____
Direct Phone _____

Yes	No	
❑	❑	**We acknowledge that our organization provides solutions or services that qualify us as a HIPAA Business Associate.**
❑	❑	**Our organization will sign HIPAA Business Associate Agreements.**
❑	❑	**Our organization signs HIPAA Business Associate Agreements with all subcontractors we work with, including cloud services, data centers, and repair services, which might access PHI.**
❑	❑	**Our organization has implemented auditable HIPAA-specific policies and procedures, completed a compliant HIPAA risk analysis and workforce training, and can provide evidence that our processes comply with HIPAA.**
❑	❑	**Our subcontractors have implemented auditable HIPAA-specific policies and procedures, completed a compliant HIPAA risk analysis and workforce training, and can provide evidence that their processes comply with HIPAA.**
❑	❑	**Our organization and subcontractors will submit to a 3rd party audit of our HIPAA compliance and that of our subcontractors.**

Comments:

I attest that the answers I have provided are correct and accurate.

_____ _____
Authorized Signature **Date**

1. **Please complete and sign this survey and send a scanned image to (name + e-mail address.)**
2. **A non-response will be considered as a 'No' answer to each question.**
3. **If you will not comply as a Business Associate we may be forced to stop working with your company.**